ABSTRACT OF THE DISCLOSURE

Disclosed is a digital certificate issuing system with intrusion tolerance ability and the issuing method thereof. The system comprises a task distributor, k calculators, m combiners and a sub-secret-key distributor. The processing of distributing a private key of a Certificate Authority comprises the steps of: the sub-secret-key distributor expressing a private key d as a sum of t sub-secret-keys d_{ji} and one sub-secret-key c_a , and t < k; the distributor distributing k×l random numbers d_{ji} into i d_{ji} per calculator and sends them to k calculators, obtaining a set of c_a and their equation combination representations and sending them to m combiners for pre-storage according to the combiner security condition. The processing of issuing certificate comprises the steps of: the task distributor sending the certificate to be signed to k calculators, the calculators computing ascending power $M^{d_{ji}}$; sending i computation results to combiners and the combiners comparing them with pre-stored equation combination representations of c_a, finding out a matched equation combination representation and obtaining corresponding c_a, and based on R obtained through multiplying $M^{d_{ji}}$, then computing M^{c_a}, obtaining a digital signature $S=M^d$, finally generating a certificate.